

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-124952**

(43)Date of publication of application : **26.04.2002**

(51)Int.Cl. **H04L 12/28**

H04Q 7/38

H04L 9/08

H04L 9/32

H04L 12/56

(21)Application number : **2000-312626**

(71)Applicant : **FURUKAWA ELECTRIC CO LTD:THE**

(22)Date of filing : **12.10.2000**

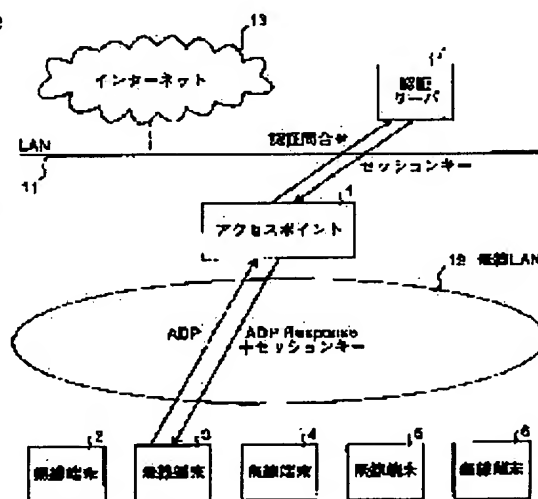
(72)Inventor : **FUKUTOMI MASASHI
OTA MASATAKA**

(54) APPROVAL METHOD AND SYSTEM OF WIRELESS TERMINAL IN WIRELESS NETWORK

(57)Abstract:

PROBLEM TO BE SOLVED: To avoid illegal access by an illegal user and illegal use of a network resource without changing a packet format.

SOLUTION: A wireless terminal (2-6) transmits a request first. A base station 1 relays the request, takes out the MAC address of the transmission origin and transmits a packet for the approval of the terminal to an approval server 7. When the approval server 7 receives the MAC address, it transmits an encoded session key. Then, the base station 1 keeps the session key and transmits the packet of the response with the session key. The wireless terminal (2-6) keeps the session key and, hereinafter, calculates a CRC value according to a HASH value obtained by adding the session key to the header and payload of the MAC, and transmits the packet. When the base station 1 receives the packet, it compares the calculated CRC value according to the HASH value with the CRC value of the packet, and realizes approval for each packet.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(11)特許出願公開番号

特開2002-124952

(P2002-124952A)

(43)公開日 平成14年4月26日(2002.4.26)

(51)Int.Cl. ⁷	識別記号	F I	データベース*(参考)	
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 B	5 J 1 0 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R	5 K 0 3 0
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C	5 K 0 3 3
9/32			6 7 5 A	5 K 0 6 7
12/56			6 7 5 D	
<div> <div>審査請求</div> <div>未請求</div> <div>請求項の数 2</div> <div>OL</div> <div>(全 6 頁)</div> <div>最終頁に続く</div> </div>				

(21)出願番号	特願2000-312626(P2000-312626)	(71)出願人	000005290 古河電気工業株式会社 東京都千代田区丸の内2丁目6番1号
(22)出願日	平成12年10月12日(2000. 10. 12)	(72)発明者	福富 昌司 東京都千代田区丸の内2丁目6番1号 古河電気工業株式会社内
		(72)発明者	太田 昌孝 東京都目黒区大岡山2-12-1
		(74)代理人	100089118 弁理士 酒井 宏明

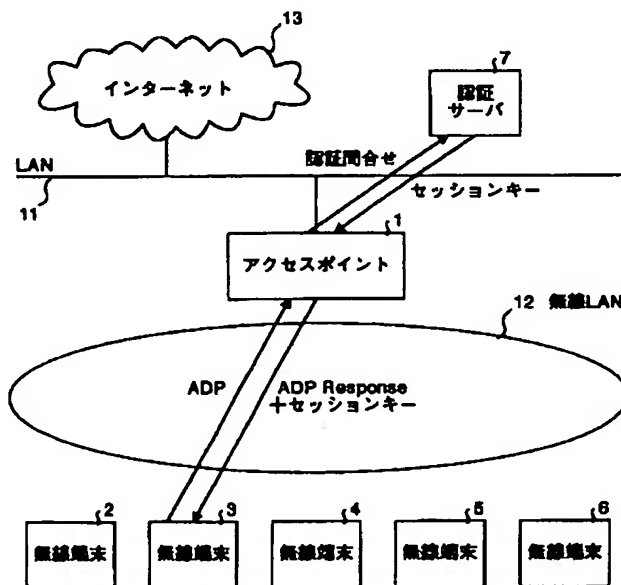
最終頁に続く

(54) 【発明の名称】 無線ネットワークにおける無線端末の認証方法および無線ネットワークにおける無線端末の認証システム

(57) 【要約】

【課題】 パケットフォーマットを変更することなく、不正なユーザによる不正アクセスを防止して、ネットワークリソースの不正利用を回避すること。

【解決手段】 無線端末2～6は、最初にリクエストを送信する。基地局1は、リクエストを中継し、送信元のMACアドレスを取り出して、端末の認証を行うためのパケットを認証サーバ7に送信し、認証サーバ7は、MACアドレスを受信すると、暗号化を行ったセッションキーを送信する。続いて、基地局1は、セッションキーを保存し、レスポンスのパケットにセッションキーをつけて送信し、無線端末2～6は、セッションキーを保存し、以降、CRC値の計算をMACのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に計算してパケット送信する。基地局1は、受信時にセッションキーを使って、HASH値を加えたCRC計算の値とパケットのCRCの値を比較してパケット単位の認証を実現する。



【特許請求の範囲】

【請求項 1】 複数の LAN と、各 LAN に対応する複数のルータまたはブリッジと、バックボーン網により構成され、各 LAN は対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各 LAN は基地局と 1 つ以上の無線端末を含む無線ネットワークにおける無線端末の認証方法であって、

前記無線端末は、最初に通信を開始するにあたり、ARP のリクエストまたは DHCP のリクエストを送信し、前記基地局は、そのリクエストを中継すると共に、送信元の MAC アドレスを取り出して、認証サーバに対して端末の認証を行うためのパケットを送信し、

前記認証サーバは、MAC アドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信し、

前記基地局は、セッションキーを保存すると共に、ARP のリプライまたは DHCP のレスポンスのパケットに、セッションキーをつけて送信し、

前記無線端末は、受信したセッションキーを保存し、以降のパケット送信では、CRC 値の計算を MAC のヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信し、

前記基地局は、パケット受信時に、保存しているセッションキーを使って、同様の HASH 値を加えた CRC 計算の値とパケットの CRC の値を比較することで、パケット単位の認証を実現することを特徴とする無線ネットワークにおける無線端末の認証方法。

【請求項 2】 複数の LAN と、無線端末の認証を行う認証サーバと、バックボーン網とにより構成され、各 LAN および認証サーバは対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各 LAN は基地局と 1 つ以上の無線端末を含む無線ネットワークにおける無線端末の認証システムであって、

前記無線端末は、最初に通信を開始する場合に、ARP のリクエストまたは DHCP のリクエストを送信する第 1 の送信手段と、前記基地局から受信したセッションキーを保存する第 1 の保存手段と、CRC 値の計算を MAC のヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信する第 2 の送信手段と、を備え、

前記基地局は、前記無線端末からのリクエストを中継すると共に、送信元の MAC アドレスを取り出して、前記認証サーバに対して端末の認証を行うためのパケットを送信する第 3 の送信手段と、前記認証サーバから受信したセッションキーを保存する第 2 の保存手段と、ARP のリプライまたは DHCP のレスポンスのパケットに、セッションキーをつけて送信する第 4 の送信手段と、パケット受信時に、前記第 2 の保存手段で保存しているセッションキーを使って、同様の HASH 値を加えた CRC 計算の値とパケットの CRC の値を比較してパケット

単位の認証を行う認証手段と、を備え、

前記認証サーバは、MAC アドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信する第 5 の送信手段を備えたことを特徴とする無線ネットワークにおける無線端末の認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の LAN と、各 LAN に対応する複数のルータまたはブリッジと、バックボーン網により構成され、各 LAN は対応するルータまたはブリッジによりバックボーン網を介して互いに接続され、各 LAN は基地局と 1 つ以上の無線端末を含む無線ネットワークにおける無線端末の認証方法および無線端末の認証システムに関する。

【0002】

【従来の技術】無線 LAN の方式は、IEEE 802.11 として標準化がなされており、アクセス方式は CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) である。基本的に端末局は自由に通信を行うことが可能であり、特に通信を開始するための認証手順はない。また、直接シーケンススペクトラム拡散方式では、利用する拡散コードを管理することで通信できる相手を特定することは可能であるが、一般に同一種類の製品では同一の拡散コードを使い、上位層の認証に利用できるような使い方はされない。

【0003】

【発明が解決しようとする課題】このような無線 LAN のシステムをアクセス網として利用する場合、契約者でない不正なユーザでも、容易にネットワークに接続することが可能であるため、ネットワークリソースの不正利用が可能であるという問題点があった。

【0004】また、不正アクセスを回避するために、パケットフォーマットに変更を行うと、データリンクの最大転送可能データ長に影響がでるため、パケットフォーマットの変更を容易に行えないという不都合もあった。

【0005】本発明は上記に鑑みてなされたものであって、パケットフォーマットを変更することなく、不正なユーザによる不正アクセスを防止して、ネットワークリソースの不正利用を回避することを目的とする。

【0006】

【課題を解決するための手段】上記の目的を達成するために、請求項 1 に係る無線ネットワークにおける無線端末の認証方法は、複数の LAN と、各 LAN に対応する複数のルータまたはブリッジと、バックボーン網により構成され、各 LAN は対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各 LAN は基地局と 1 つ以上の無線端末を含む無線ネットワークにおける無線端末の認証方法であって、前記無線端末は、最初に通信を開始するにあたり、ARP のリクエ

ストまたはDHCPのリクエストを送信し、前記基地局は、そのリクエストを中継すると共に、送信元のMACアドレスを取り出して、認証サーバに対して端末の認証を行うためのパケットを送信し、前記認証サーバは、MACアドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信し、前記基地局は、セッションキーを保存すると共に、ARPのリプライまたはDHCPのレスポンスのパケットに、セッションキーをつけて送信し、前記無線端末は、受信したセッションキーを保存し、以降のパケット送信では、CRC値の計算をMACのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信し、前記基地局は、パケット受信時に、保存しているセッションキーを使って、同様のHASH値を加えたCRC計算の値とパケットのCRCの値を比較することで、パケット単位の認証を実現することを特徴とする。

【0007】この発明によれば、IPでの通信を開始するにあたり、無線端末が、ARPのリクエストまたはDHCPのリクエストを送信する。基地局（アクセスポイント）側では、このARPまたはDHCPパケットの送信元MACアドレスを取り出して、認証サーバに対して端末の認証を依頼する。認証サーバは、MACアドレスをチェックし、あらかじめ配布しているシークレットキーで暗号化したセッションキーを送信し、基地局は、セッションキーを保存すると共に、ARPのリプライまたはDHCPのレスポンスパケットにセッションキーをつけて送信する。無線端末は、受信したセッションキーを保存し、端末局はセッションキー入手以降、パケット送信時に、MACフレームのCRCの値を計算するにあたって、MACヘッダ、ペイロードとセッションキーでHASH値を計算し、そのHASH値がペイロードの最後に付加されたパケットに対してCRCを計算し、そのCRC値を通常のMACフレームのCRC値として送信を行う。基地局では、このパケットを受信した場合、受信したパケットのMACヘッダとペイロードとセッションキーから端末側の処理と同様にHASH値を計算し、それを加えてCRC値の計算を行い、受信したパケットのCRC値と比較を行って、パケット単位の認証を行う。したがって、パケット単位での認証が可能であり、事前に共有するセッションキーはパケットからは判別できないことから、無線ネットワーク上のパケットを盗み見て、なりすましによる不正アクセスを防止することが可能になる。また、パケットフォーマットに変更を行わないので、データリンクの最大転送可能データ長に影響を与えることはなく、利用者にはトランスペアレントである。

【0008】また、請求項2に係る無線ネットワークにおける無線端末の認証システムは、複数のLANと、無線端末の認証を行う認証サーバと、バックボーン網とに

より構成され、各LANおよび認証サーバは対応するルータまたはブリッジにより前記バックボーン網を介して互いに接続され、各LANは基地局と1つ以上の無線端末を含む無線ネットワークにおける無線端末の認証システムであって、前記無線端末は、最初に通信を開始する場合に、ARPのリクエストまたはDHCPのリクエストを送信する第1の送信手段と、前記基地局から受信したセッションキーを保存する第1の保存手段と、CRC値の計算をMACのヘッダ、ペイロードにセッションキーを加えたハッシュ値を元に、計算してパケットを送信する第2の送信手段と、を備え、前記基地局は、前記無線端末からのリクエストを中継すると共に、送信元のMACアドレスを取り出して、前記認証サーバに対して端末の認証を行うためのパケットを送信する第3の送信手段と、前記認証サーバから受信したセッションキーを保存する第2の保存手段と、ARPのリプライまたはDHCPのレスポンスのパケットに、セッションキーをつけて送信する第4の送信手段と、パケット受信時に、前記第2の保存手段で保存しているセッションキーを使って、同様のHASH値を加えたCRC計算の値とパケットのCRCの値を比較してパケット単位の認証を行う認証手段と、を備え、前記認証サーバは、MACアドレスを受信すると、あらかじめ配布しているシークレットキーで暗号化を行ったセッションキーを送信する第5の送信手段を備えたことを特徴とする。

【0009】

【発明の実施の形態】以下、本発明の無線ネットワークにおける無線端末の認証方法および無線端末の認証システムの一実施の形態について図面を参照して詳細に説明する。

【0010】図1は、本発明の一実施の形態のネットワーク説明図である。本実施の形態のネットワークはLAN11と無線LAN12とインターネット13により構成され、LAN11と無線LAN12は、アクセスポイント1を介して互いに接続されている。なお、無線LAN12は、アクセスポイント1と無線端末2, 3, 4, 5, 6から構成される。LAN11はアクセスポイント1と認証サーバ7から構成される。

【0011】図2は、図1のネットワークを構成する無線端末2～6の構成を示すブロック図である。無線端末2～6は、記憶装置21とCRC計算部22とパケット処理部23と無線通信部24とを備えている。記憶装置21には、無線端末のMACアドレスと無線端末が通信する場合に利用するセッションキーを格納する。

【0012】CRC計算部22は、パケット処理部がパケット送信において、パケットにつけるCRCの計算を行う。CRCの計算は、図4に示すように、送信するパケットのMACヘッダとペイロードの部分とセッションキーの値を含めて、HASH値の計算を行い、そのHASH値を送信パケットのMACヘッダとペイロード部分

10

20

30

40

50

の後に入れた形で、パケットのCRC値計算を行う。

【0013】パケット処理部23は、パケットの送受信を行うが、パケットの送信時に、前記のCRC計算部で計算したCRC値をパケットのCRCの部分に添付して送信を行う。

【0014】無線通信部24は、パケット部から送信パケットを受け、無線LANに対して送信処理を行い、また、無線LANから受信するパケットをパケット処理部に通知する。

【0015】図3は、図1のネットワークを構成するアクセスポイント1の構成を示すブロック図である。アクセスポイント1は、LAN通信部31とパケット処理部32と無線通信部34と記憶装置34とCRC計算部35とを備える。LAN通信部31は、アクセスポイント1が接続しているLAN11へのパケットの送受信を制御する。パケット処理部32は、LAN11から受信したパケットを、無線LAN12へ中継する処理を行う、また無線LAN12から受信したパケットをLAN11に中継する。

【0016】アクセスポイント1では、無線LAN12からパケットを受信した場合に、図4で無線端末が行う処理とは逆の処理を行う。受信において、MACヘッダとペイロードの部分とセッションキーの値を含めてHASH値の計算を行い、そのHASH値を送信パケットのMACヘッダとペイロード部分の後に入れた形で、パケットのCRC計算を行って、受信パケットに含まれていたCRCの値と一致するかどうかを確認する。一致する場合には、受信パケットをLAN11に中継し、一致しない場合には、廃棄する。この動作により、セッションキーを持たない無線端末が無線LANネットワークを利用して、インターネットへの接続を行うことを排除することが可能になる。

【0017】前述したように本実施の形態によれば、パケット単位での認証が可能であり、かつ、事前に共有するセッションキーはパケットからは判別できないため、無線ネットワーク上のパケットを盗み見て、なりすましによる不正アクセスを防止することができる。また、パケットフォーマットに変更を行わないので、データリンクの最大転送可能データ長に影響を与えることはなく、利用者にはトランスペアレントであるという効果を奏する。

【0018】さらに、セッションキーをARPやDHCPなどのリンク層以上のプロトコルのパケットに追加することによって、認証のためのトラフィックを増加を抑制することで、接続時間の短縮を行うことが可能となる。

【0019】

【発明の効果】以上説明したように、本発明（請求項1および請求項2）によれば、IPでの通信を開始するにあたり、無線端末が、ARPのリクエストまたはDHCPのリクエストを送信し、基地局（アクセスポイント

側）では、このARPまたはDHCPパケットの送信元MACアドレスを取り出して、認証サーバに対して端末の認証を依頼し、認証サーバが、MACアドレスをチェックし、あらかじめ配布しているシークレットキーで暗号化したセッションキーを送信し、基地局では、セッションキーを保存すると共に、ARPのリプライまたはDHCPのレスポンスパケットにセッションキーをつけて送信し、無線端末が、受信したセッションキーを保存し、端末局はセッションキー入手以降、パケット送信時に、MACフレームのCRCの値を計算するにあたって、MACヘッダ、ペイロードとセッションキーでHASH値を計算し、そのHASH値がペイロードの最後に付加されたパケットに対してCRCを計算し、そのCRC値を通常のMACフレームのCRC値として送信を行い、基地局では、このパケットを受信した場合、受信したパケットのMACヘッダとペイロードとセッションキーから端末側の処理と同様にHASH値を計算し、それを加えてCRC値の計算を行い、受信したパケットのCRC値と比較を行って、パケット単位の認証を行うため、パケット単位での認証が可能であり、かつ、事前に共有するセッションキーはパケットからは判別できないことから、無線ネットワーク上のパケットを盗み見て、なりすましによる不正アクセスを防止することが可能になる。また、パケットフォーマットに変更を行わないので、データリンクの最大転送可能データ長に影響を与えることはなく、利用者にはトランスペアレントである。換言すれば、パケットフォーマットを変更することなく、不正なユーザによる不正アクセスを防止して、ネットワークリソースの不正利用を回避することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態のネットワーク説明図である。

【図2】図1のネットワークを構成する無線端末2～6の構成を示すブロック図である。

【図3】図1のネットワークを構成するアクセスポイント1の構成を示すブロック図である。

【図4】無線端末の送信時の処理であるCRCの計算を示す説明図である。

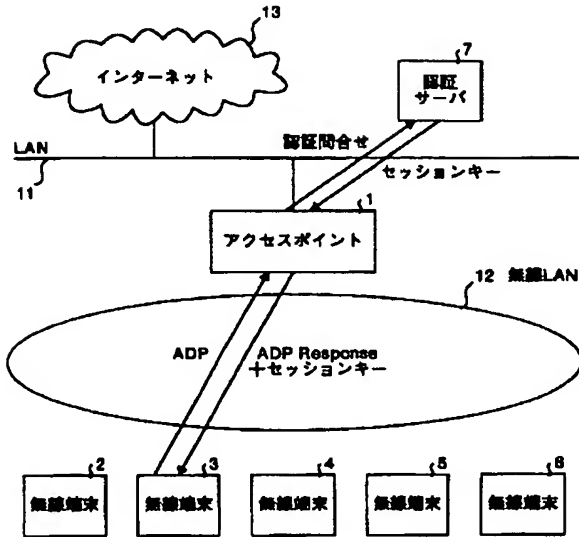
【符号の説明】

- 1 アクセスポイント
- 2, 3, 4, 5, 6 無線端末
- 7 認証サーバ
- 11 LAN
- 12 無線LAN
- 13 インターネット
- 21 記憶装置
- 22 CRC計算部
- 23 パケット処理部
- 24 無線通信部
- 31 LAN通信部

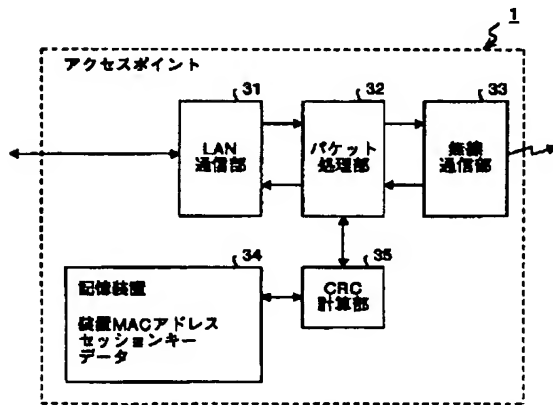
32 パケット処理部
33 無線通信部

34 記憶装置
35 CRC計算部

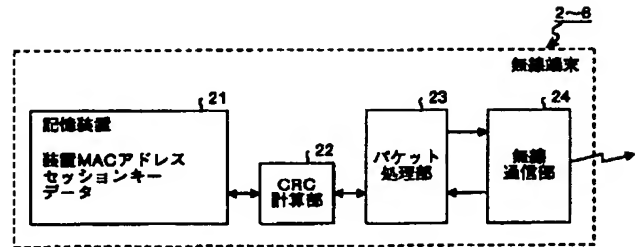
【図1】



【図3】



【図2】

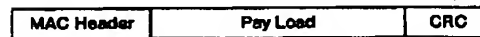
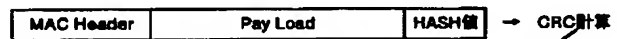


【図4】

無線端末局送信時の処理



MAC Header+Pay Load+セッションキー → HASH値計算



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I
H 0 4 L 11/20

テーマコード(参考)

1 0 2 Z

F ターム(参考) 5J104 AA07 AA16 EA04 EA18 EA22
KA02 KA06 MA01 NA03 NA12
PA01
5K030 GA15 HA08 HB12 HB28 HC14
HD03 HD07 JL01 LD19
5K033 AA08 CA08 DA05 DA17
5K067 AA30 BB21 CC08 DD13 DD17
DD51 EE02 EE10 HH23 HH26
HH36 KK15